Channeler Requirements for the Departmental Order Process

June 10, 2011

This document provides requirements for FBI-approved Channelers (Channelers) processing the electronic submissions of the United States (U.S.) Department of Justice Order (DO) 556-73 (DO 556-73) requests. This document, along with the *CJIS Security Policy*, Channeler contract addendum, and the pertinent sections of the Security and Management Control Outsourcing Standard for Channelers (Outsourcing Standard for Channelers), shall be adhered to at all times by a Channeler while processing DO 556-73 requests. Additional questions may be directed to [redacted] b6 b7C or via e-mail at [redacted]

I. Background

The federal regulations pertaining to the DO 556-73 process are found at 28 Code of Federal Regulations 16.30-16.34. These regulations establish procedures to be followed when an individual subject of an FBI criminal identification record requests production of that record to review it or obtain a change, correction, or updating of that record. The FBI CJIS Division currently processes all DO 556-73 requests and the specific procedures and forms may be found on the FBI's website (www.fbi.gov).

Under DO 556-73, an individual may obtain a copy of his/her FBI criminal identification record, upon request, for review and correction purposes, to challenge the information on record, or satisfy certain legal requirements such as a requirement for adopting a child; to satisfy a requirement to live in a foreign country; to satisfy a requirement to work in a foreign country; to satisfy a requirement to travel in a foreign country; and/or other court-related matters.

Pursuant to the regulations and FBI policy, the current procedures for an individual requesting a copy of his/her criminal identification record are as follows:

1) Complete and submit the written information form;
2) Obtain and submit a complete set of the individual's fingerprints;
3) Submit $18[1] (U.S.) per request, via money order, cashier check or credit card, made payable to the Treasury of the U.S.;
4) Review the FBI criminal identification records request checklist; and
5) Mail the above items to the FBI Criminal Justice Information Services (CJIS) Division.

The FBI CJIS Division ensures that all information is complete, and returns a response to the address provided by the individual.

II. Policy Requirements

A Channeler with the intention of processing DO 556-73 requests is expected to follow the same regulatory and policy requirements regarding the receipt of the written information form, complete set of fingerprints, and appropriate fee from the individual.

[1] Fee must be for the exact amount and is established pursuant to the provisions of 31 U.S.C. 9701.

A Channeler submitting DO 556-73 transactions on behalf of individuals must first request a unique Originating Agency Identifier (ORI) from the FBI. After a Channeler has requested and acquired a unique ORI for processing DO 556-73 requests, there are specific security and privacy requirements that must be maintained and adhered to for processing DO 556-73 requests at all times.

Compliance with the requirements listed in the most current versions of the Outsourcing Standard for Channelers and the *CJIS Security Policy* will ensure that a Channeler complies with site security, personnel security, data security, system security and dissemination safeguards. The following sections of the Outsourcing Standard for Channelers are mandatory requirements for processing DO 556-73 requests:

- Section 2.03(a)
- Section 2.03(b)
- Section 2.03(c)
- Section 2.05
- Section 3.01
- Section 3.02
- Section 3.03
- Section 3.06
- Section 3.08
- Section 3.09
- Section 4.01
- Section 4.02
- Section 5.0 (Dissemination)
- Section 6.0 (Personnel Security)
- Section 7.0 (Site Security)
- Section 8.0 (Security Violations)

A. Processing DO 556-73 Requests

1) A Channeler may only submit requests for a U.S. person (who is a citizen of the U.S. or a lawful permanent resident of the U.S.).

2) The fingerprint submission must include the individual's complete legal name (to include first, middle, and last name); date of birth; signature (if applicable); descriptive data, such as sex, race, gender; date fingerprinted; and the reason fingerprinted (RFP). The RFP literal must state "**DO 556-73 REQUEST**."

3) A Channeler shall ensure the fingerprint submission includes ten rolled fingerprint impressions and ten plain fingerprint impressions or ten flat fingerprint impressions segmented as outlined in the Electronic Biometric Transmission Specification (EBTS), Version 9.1, released on May 25, 2010, or the most current version.

4) Each fingerprint submission must be accompanied by a signed DO Request Form, filled out in its entirety, from the individual seeking his/her FBI criminal identification record pursuant to DO 566-73. DO Request Forms will be provided to the Channeler by the FBI and a copy of the form is enclosed. A Channeler may change the format of the DO Request Form; however, all necessary information must be included on the Channeler's version of the form. Should a Channeler desire to make changes to the provided DO Request Form, the FBI must review and approve these changes prior to use. Any and all subsequent revisions must also be reviewed and approved by the FBI prior to use.

5) A Channeler must maintain each DO Request Form with the original signature from each individual, for a period of three (3) years or upon termination of the contract, whichever is shorter. Maintenance of the DO Request Forms may be in digitized or hard copy format.

6) At the end of the mandatory retention period, all DO Request Forms must be destroyed in accordance with the provisions outlined in the most current versions of the Outsourcing Standard for Channelers (currently Sections 7.02 (b) and (c)) and the *CJIS Security Policy* for fixed storage media and disposal of all non-fixed storage media of criminal history record information (CHRI).

7) Fingerprints must be captured by a law enforcement agency or Channeler. An individual may not capture his/her own fingerprints on a fingerprint card.

8) If an individual submits fingerprints in person through a Channeler or other entity authorized by a Channeler, the following requirements must be met:
   a) The individual's identity must be verified by two forms of identification (at least one of which must be a government issued photo ID).
   b) The mailing address of the individual making the request must match at least one form of identification provided to a Channeler as listed on the DO Request Form.

9) If a DO 556-73 request is made through an attorney, the request shall be submitted on attorney letterhead with both the individual and the attorney signatures, and shall contain a release statement.

10) Fingerprint cards and fingerprint images used for submission of DO 556-73 requests may not be retained by a Channeler for a period longer than 30 calendar days or upon successful dissemination, whichever is shorter. All fingerprint cards and images must be destroyed/deleted in a manner meeting the same criteria as destruction of CHRI listed in the Outsourcing Standard for Channelers (currently Sections 7.02 (b) and (c)).

11) The same fingerprint images may not be used for more than one submission per individual. In case of fingerprint quality rejects, a Channeler should initially obtain two sets of fingerprint images for an individual for resubmission purposes.

B. Restricted Requests

1) An individual requiring an apostille[2] or authenticated copy of his/her FBI criminal identification record must submit a request directly to the FBI CJIS Division for processing.

2) Any non U.S. person making a request for his/her FBI criminal identification record must submit his/her request directly to the FBI CJIS Division to be processed.

3) Should a Channeler be contacted to obtain an FBI criminal identification record for an individual requesting an apostille or a non U.S. person, the Channeler is required to instruct the individual to follow the instructions provided on the FBI website.

C. Fingerprint Submissions

The FBI CJIS Division utilizes the EBTS for Data Format for the Interchange of Fingerprints and related data. The EBTS Version 9.1, released on May 25, 2010, is the latest upgrade. Due to the increased emphasis placed on communicating interface formats and guidelines, Integrated Automated Fingerprint Identification System (IAFIS) users are encouraged to register with the website below to receive future notifications on FBI Biometric Standards, Next Generation Identification capability implementation details, and EBTS updates. When updates are made to the EBTS, the version number will change using a sequential version release numbering scheme. A copy of the EBTS may be obtained at the following website: <www.fbibiospecs.org>.

The minimum record set includes Type 1, 2, and 4 or 14 records for each submission. All EBTS mandatory fields must be complete. In addition, the following EBTS fields should contain the provided data elements to meet the requirements for DO 556-73 requests:

1.004 TOT Type of Transaction - Must be **DOCE**.

1.007 DAI Destination Agency Identifier - Must contain the value [redacted] NOTE: The character before the Z is a numeric zero (0). b7E

1.008 ORI Originating Agency Identifier - Must contain the ORI specifically assigned to the Channeler for the Departmental Order process.

[2] An apostille is a certification that a document that has been "legalized" or "authenticated" by the issuing agency through a process in which various seals are placed on the document.

1.009 TCN Transaction Control Number - This is a unique number assigned to the record by a Channeler.

1.010 TCR Transaction Control Reference field - This field shall be used in responses only to refer to the TCN of a previous transaction involving an inquiry or other action that required a response. For resubmissions due to poor image quality, use the received TCN in the TCR field.

2.005 RET Retention Code - "N" for No.

2.037 RFP Reason Fingerprinted - Must use "**DO 556-73 REQUEST**".

2.070 RAP Rap Sheet - Request for Electronic Rap Sheet - "Y" for Yes.

2.073 CRI Controlling Agency Identifier - Must enter the same ORI identifier that is used in the ORI field.

A Channeler must assign a unique number for each individual to identify and track submissions, send responses, and collect fees. The FBI CJIS Division recommends using the Originating Agency Case (OCA) Number (2.009) field or the second occurrence of the CRI (2.073) field. The OCA alphanumeric-special field contains one to twenty characters and any printable 7-bit ASCII character with the exception of the period (.) or a blank in the first position. The second CRI field must be a nine-byte alphanumeric field.

All DO 556-73 submissions will be sent to the FBI via a separate host Internet Protocol (IP) address associated with the DO 556-73 ORI. The "DOCE" TOT is the only type of submission that shall be submitted to the FBI through the IP address.

D. Hot Check Notifications

The FBI CJIS Division conducts automated name-based searches ("Hot Check") of the National Crime Information Center Files on all ten-print fingerprint submissions.

Law Enforcement agencies may contact a Channeler for an individual's information (e.g., address information) if the agency receives information through the FBI's Hot Check service.

A Channeler must not advise the individual of a law enforcement request!

E. Fingerprint Responses

1) The FBI's IAFIS will process each transaction and send the Channeler an IAFIS Tenprint Response, the Submission Results-Electronic (SRE). The SRE will contain the ident/non-ident response, the rap sheet (when applicable), or a Reject Message (ERRT). A list of ERRT's can be found in the EBTS. Sample SREs are available upon request.

2) A Channeler shall expeditiously disseminate the criminal history record (CHR) check results to the individual seeking his/her FBI criminal identification record or the individual's attorney as specified in the Outsourcing Standard for Channelers (currently Section 5.0). All electronic dissemination (email or through a website) must meet or exceed the requirements outlined in the *CJIS Security Policy* for encryption. CHRI disseminated by a Channeler to an individual via an authorized website shall remain on such website only for the time necessary to meet the individual's requirements but in no event shall that time exceed 30 calendar days.

3) All FBI responses shall be provided to the individual in the exact format it was received by a Channeler with no deviation or changes made to the document(s).

4) A Channeler shall establish a system that ensures that each SRE and rap sheet (when applicable), either paper or electronic, cannot be altered or copied without detection. A Channeler shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations.

5) A Channeler's security system shall comply with the *CJIS Security Policy* and the Outsourcing Standard for Channelers. A Channeler is responsible for protecting CHRI with firewall-type devices for the prevention of unauthorized access. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

6) CHRI shall be destroyed by a Channeler immediately after confirmation of successful receipt by the individual, regardless of mode. CHRI must be destroyed in compliance with the criteria in the Outsourcing Standard for Channelers (currently Sections 7.02 (b) and (c)). The manner and time period for CHRI dissemination by a Channeler to an individual shall be defined in the relevant contract.

F. Resubmission Guidelines

If a DO 556-73 submission rejects for fingerprint image quality, a second submission of the same individual may be processed at no charge by following the FBI CJIS Division's resubmission guidelines. A Channeler must place the received TCN (1.009) field from the electronic fingerprint response of the original rejected

submission in the TCR (1.010) field of the new submission. The second submission must be within one calendar year after the original fingerprint submission was rejected. Name checks will not be permitted, regardless of reason(s).

For additional information, please contact the FBI CJIS Division Customer Service Group (CSG) at (304) 625-5590 (8 a.m. – 12 a.m., Monday-Friday, Eastern Standard Time (EST)).

G. Personally Identifiable Information (PII) Breaches

The FBI and all federal executive agencies define PII as "information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name." Therefore, the DO Request Form, the fingerprint card, and the SRE for an individual (to include the rap sheet) all contain PII. Other information submitted by the individual may also contain PII, such as personal information provided when making payment for a DO 556-73 request.

A PII breach occurs when there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any situation where persons other than the authorized users, and for other than authorized purposes, have access or potential access to PII, whether physical or electronic. A PII breach may be accidental or purposeful.

Pursuant to the Department of Justice (DOJ) Memorandum, the loss of any sensitive FBI information must be reported to the FBI immediately so steps may be taken to investigate and mitigate the loss. The FBI is required to report breaches to the DOJ within one hour of discovery of the loss. Because of these requirements, it is necessary for a Channeler to contact the FBI CJIS Division as soon as any PII breach occurs so that the FBI may determine the severity of the breach and the associated reporting requirements. All PII breaches or questions concerning possible PII breaches may be directed to the CSG by calling (304) 625-5590 and requesting to speak with a PII point of contact.

A Channeler is responsible for protecting all PII in its possession and control during the processing of DO 556-73 requests. In addition, a Channeler should notify the individual making the DO 556-73 request of his/her right (via language approved by the FBI) to report PII breaches to the FBI should he/she believe personal information has been compromised.

H. Financial Requirements

For each DO 556-73 submission to the FBI CJIS Division, a Channeler will be billed $18. (All FBI fees are subject to change.) Channelers will be notified in writing of billing changes ninety (90) days prior to the effective date.

A Channeler shall submit payment to the FBI within thirty (30) calendar days from the invoice date. A Channeler shall be responsible for all collections from an individual making a CHR check through the DO 556-73 process. The FBI CJIS Division will not assist a Channeler in collecting "bad" debts or grant billing adjustments for any such failed collection.

The Channeler should contact the CJIS Division CSG at (304) 625-5590 to address potential billing errors as early as possible.

I. Audits

1) The FBI shall conduct an audit of a Channeler within 90 days of the date a Channeler first receives CHRI under the terms of the Outsourcing Standard for Channelers. In addition, the FBI shall conduct one year and triennial audits of a Channeler thereafter.

2) A Channeler shall provide all logs required to be maintained by a Channeler as listed in the Outsourcing Standard for Channelers to the FBI during announced and unannounced audits, to include but not limited to, dissemination of CHRI.

3) The FBI Compact Officer, National Crime Prevention and Privacy Compact Council (Compact Council), and the U.S. Attorney General reserve the right to audit a Channeler's operations and procedures at scheduled or unscheduled times.

4) The Compact Council and the U.S. Attorney General are authorized to perform a final audit of a Channeler's system after termination and/or conclusion of the DO 556-73 contract between the FBI and a Channeler.

J. Security Requirements

A Channeler shall develop, document, administer, and maintain a Security Program (to include physical, personnel, and information technology) that complies with the most current versions of the Outsourcing Standard for Channelers and the *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in the Outsourcing Standard for Channelers and the *CJIS Security Policy*. In addition, the Channeler is also responsible to set, maintain,

and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The FBI shall provide the written approval of a Channeler's Security Program.

The requirements for a Security Program should include, at a minimum:
a) description of the implementation of the security requirements explained in the Outsourcing Standard for Channelers and the *CJIS Security Policy*,
b) security training,
c) guidelines for documentation of security violations, and
d) standards for the selection, supervision, and separation of personnel with access to CHRI.
**If a Channeler follows a corporate security policy, it must meet or incorporate the requirements outlined in the Outsourcing Standard for Channelers and the *CJIS Security Policy*.

The FBI shall ensure that a Channeler's site is a physically secure location to protect against unauthorized access to CHRI. All visitors to computer centers and/or terminal areas shall be escorted by authorized personnel at all times.

The FBI shall conduct criminal history record checks of Channeler (and approved sub-contractor) personnel having access to CHRI. A Channeler shall confirm in writing that each employee has certified that he/she understands all requirements and laws that apply to his/her responsibilities. Criminal history record checks and the certification must be completed prior to accessing CHRI.

All Channeler (and approved sub-contractor) personnel must complete, and verify to the FBI, any mandatory training provided by the FBI. A list of Channeler personnel who have access to CHRI shall be maintained by the FBI, with updates provided by the Channeler within 24 hours to the FBI when changes occur. All access to, and dissemination of, CHRI and associated PII is for official purposes only.

If CHRI can be accessed via Wide Area Network/Local Area Network or the Internet, then the Channeler shall protect the CHRI with firewall-type devices to prevent unauthorized access. In addition, data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

An up-to-date log concerning dissemination of CHRI shall be maintained by a Channeler for a minimum one year retention period. This log must clearly identify: (a) the individual and the secondary recipient, with assigned unique identifying numbers; (b) the record disseminated; (c) the date of dissemination; (d) the statutory authority for dissemination; and (e) the means of dissemination.

If CHRI is stored or disseminated in an electronic format, a Channeler shall protect against any unauthorized persons gaining access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than

governed by the Outsourcing Standard for Channelers or more stringent contract requirements.

All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity. A Channeler's system shall be supported by a documented contingency plan as defined in the *CJIS Security Policy* and approved by the FBI.

A Channeler shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel. The FBI shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract. The FBI shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies).

A Channeler shall maintain a written policy for discipline of employees who violates any security or privacy provisions of these requirements, the relevant contract, the Outsourcing Standard for Channelers, and the *CJIS Security Policy*. A Channeler shall not permit any employee suspected of committing a violation to have access to CHRI.

A Channeler shall immediately (within four hours) notify the FBI and/or individual of any security violation to include unauthorized access to CHRI. Within five calendar days of such notification, the Channeler shall provide the FBI and/or individual with a written report documenting such security violation, any corrective actions taken by the Channeler to resolve such violation, and the date, time, and summary of the prior notification. Each individual shall be provided information regarding a means of notifying the FBI of any security violation (to include unauthorized access to CHRI).

The FBI Compact Officer, Compact Council and the U.S. Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

K. Causes for Contract Termination

1. Failure to comply with any applicable federal law or regulation, as well as all requirements and policies explained in this document.

2. Notifying an individual of a law enforcement agency inquiry regarding an NCIC hot check notification.

3. Knowingly processing DO 556-73 requests for individuals who are not U.S. persons.

4. Knowingly processing DO 556-73 requests for employment and/or licensing purposes.

5. Knowingly processing DO 556-73 requests that require an apostille or authenticated copy of an individual's record.

6. Advertising, soliciting, proposing, or utilizing the DO 556-73 process for employment and/or licensing or any other unauthorized purpose.

7. Submitting a name check for an individual requesting a DO 556-73 request.

III. Information Resources/Training

For fingerprint processing questions (i.e., submission status inquiries, rejections), please contact the FBI CJIS CSG at (304) 625-5590 (8 a.m. – 12 a.m., Monday-Friday, EST).

For policy and procedural questions, please contact [redacted] at [redacted] or via e-mail at <[redacted]>

b6
b7C

For technical or hardware issues (i.e., management of lines, connection problems), please contact the FBI CJIS Division Help Desk at (304) 625-4357 (24 hours a day, 7 days a week).

Limited courses are offered by the FBI on "Fingerprint and CHR Training" and "Recording Legible Fingerprints." Requests for such courses may be sent to <liaison@leo.gov> for more information.